Incident response tools

As a security analyst, you'll play an important role in incident detection.
After all, you're going to be at the front lines actively detecting threats.
To do this, you'll not only rely on the security knowledge you've developed so far,
but you'll also be using a variety of tools and technologies to support your investigations.

A great carpenter doesn't just use a hammer to create a piece of furniture.
They rely on a variety of tools in their toolbox to get the job done.
They'll need to use a tape measure to measure dimensions, a saw to cut wood, and sandpaper to smooth the surface.

Likewise, as a security analyst, you won't be using a single tool to monitor, detect, and analyze events.
You'll use detection and management tools to monitor system activity to identify events that require investigation.
You'll use documentation tools to collect and compile evidence.
And you'll also use different investigative tools for analyzing these events, like packet sniffers.
New security technologies emerge, threats evolve, and attackers become stealthier to avoid detection.
To become effective at detecting threats, you'll need to continuously expand your security toolbox.
That's what makes the security field such an exciting one to be in.
There's always something new to be learned.

You might remember the incident handler's journal we shared with you from the previous section.
You'll be using this journal as your own form of documentation as you work through the rest of this course.
Consider this to be your first security tool to add to your toolbox.

Revision #1
Created 6 September 2023 10:56:35 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai